

# MoveFile

Indeterminate whether expected ACL exists on file after move (function is deprecated)

Sean Barnum, Digital, Inc. [vita<sup>1</sup>]

Copyright © 2007 Digital, Inc.

2007-04-02

## Part "Original Digital Coding Rule in XML"

Mime-type: text/xml, size: 3940 bytes

<b>Attack Category</b>	<ul style="list-style-type: none"><li>• Privilege Exploitation</li><li>• Path spoofing or confusion problem</li></ul>									
<b>Vulnerability Category</b>	<ul style="list-style-type: none"><li>• Access Control</li></ul>									
<b>Software Context</b>	<ul style="list-style-type: none"><li>• File Management</li></ul>									
<b>Location</b>	<ul style="list-style-type: none"><li>• winbase.h</li></ul>									
<b>Description</b>	<p>The MoveFile function moves an existing file or a directory, including its children.</p> <p>There is ambiguity whether the expected ACL will exist for the destination file after the move.</p>									
<b>APIs</b>	<table border="1"><thead><tr><th>Function Name</th><th>Comments</th></tr></thead><tbody><tr><td>MoveFile</td><td></td></tr><tr><td>MoveFileA</td><td></td></tr><tr><td>MoveFileW</td><td></td></tr></tbody></table>		Function Name	Comments	MoveFile		MoveFileA		MoveFileW	
Function Name	Comments									
MoveFile										
MoveFileA										
MoveFileW										
<b>Method of Attack</b>										
<b>Exception Criteria</b>										
<b>Solutions</b>	<b>Solution Applicability</b>	<b>Solution Description</b>	<b>Solution Efficacy</b>							
	Always	In general the only real problem here appears to be one of deprecation.  Use SHFileOperation instead of MoveFile to ensure that the expected ACL is in place for the destination file.	Effective							

1. [http://buildsecurityin.us-cert.gov/bsi/about\\_us/authors/35-BSI.html](http://buildsecurityin.us-cert.gov/bsi/about_us/authors/35-BSI.html) (Barnum, Sean)

<b>Signature Details</b>	BOOL MoveFile(LPCTSTR lpExistingFileName,LPCTSTR lpNewFileName);				
<b>Examples of Incorrect Code</b>	<pre>if (MoveFileEx(old, new, MOVEFILE_REPLACE_EXISTING) != TRUE) ret = GetLastError();</pre>				
<b>Examples of Corrected Code</b>	<pre>SHFILEOPSTRUCT dirmove; memset(&amp;dirmove, 0, sizeof(SHFILEOPSTRUCT)); dirmove.wFunc = FO_MOVE; dirmove.pFrom = tsrc; dirmove.pTo = tdest; dirmove.fFlags = FOF_NOCONFIRMATION   FOF_SIMPLEPROGRESS; dirmove.hNameMappings = 0; dirmove.lpszProgressTitle = copytitle; if(SHFileOperation(&amp;dirmove)==0) ret = TRUE;</pre>				
<b>Source References</b>	<ul style="list-style-type: none"> <li>• <a href="http://msdn.microsoft.com/library/default.asp?url=/library/en-us/shellcc/platform/Shell/programmersguide/sec_shell.asp">http://msdn.microsoft.com/library/default.asp?url=/library/en-us/shellcc/platform/Shell/programmersguide/sec_shell.asp</a><sup>2</sup></li> <li>• Lucersoft. <a href="#">MoveFile</a><sup>3</sup>(2003).</li> <li>• <a href="http://msdn.microsoft.com/library/default.asp?url=/library/en-us/fileio/fs/movefile.asp">http://msdn.microsoft.com/library/default.asp?url=/library/en-us/fileio/fs/movefile.asp</a><sup>4</sup></li> </ul>				
<b>Recommended Resource</b>					
<b>Discriminant Set</b>	<table border="1"> <tr> <td><b>Operating System</b></td><td>• Windows</td></tr> <tr> <td><b>Languages</b></td><td>• C • C++</td></tr> </table>	<b>Operating System</b>	• Windows	<b>Languages</b>	• C • C++
<b>Operating System</b>	• Windows				
<b>Languages</b>	• C • C++				

## Cigital, Inc. Copyright

Copyright © Cigital, Inc. 2005-2007. Cigital retains copyrights to this material.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

For information regarding external or commercial use of copyrighted materials owned by Cigital, including information about “Fair Use,” contact Cigital at [copyright@cigital.com](mailto:copyright@cigital.com)<sup>1</sup>.

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

---

1. <mailto:copyright@cigital.com>